REMARKS

In the Advisory Action mailed on **16 May 2007**, the Examiner reviewed claims 1-4, 6-13, 15-22, and 24-30. Claims 1, 10 and 19 were rejected under 35 U.S.C. § 112. Claims 1-4, 6-13, 15-22 and 24-30 were rejected under 35 U.S.C. § 102(b) based on Hermann (EPO Pub No EP1024626A1, hereinafter "Hermann").

Rejections under 35 U.S.C. §112

Claims 1, 10 and 19 were rejected under 35 U.S.C. § 112 as failing to comply with the written description requirement. Specifically, the Examiner avers that the amended negative limitation "**wherein the preferred channel does not require being resistant to eavesdropping**" is not disclosed by the specification of the instant application.

Applicant respectfully recites page 19, paragraph [0078] of the specification below:

"**[0078]** One skilled in the art will understand that the commitment to the key is transferred over the preferred channel because the preferred channel is assumed to be resistant to undetected active attacks and to thereby endow data transferred across it with the authenticity property. **A channel does not need to be resistant to eavesdroppers to be used as a preferred channel because only public information (e.g., a public key, or a commitment to a public key) is sent over that channel**; a pair of devices authenticating themselves to each other by sending such key or commitment information over the preferred channel are able to set up a secure communication with each other because they can demonstrate possession of the private keys corresponding to the public keys committed to or exchanged over the preferred channel (using any technique known in the art, such as a key exchange protocol like SSLSTLS). An eavesdropper that detects the commitment or keys sent across the preferred channel is not able to demonstrate possession of the corresponding private key,

and therefore is unable to affect communication between the legitimate parties. Further, one skilled in the art will understand that the preferred channel can be a very low bandwidth channel as only needs to carry the key commitment (and possibly essential communication parameters for the non-preferred channel -- such as a LAN, or Internet). The provisioning of the credential and other information to the prospective member device can be accomplished using the non-preferred channel(s)."

Hence, the specification of the instant application explicitly and literally discloses the negative limitation "**wherein the preferred channel does not require being resistant to eavesdropping**."

Rejections under 35 U.S.C. §102(b)

Independent claims 1, 10, and 19 were rejected as being anticipated by Hermann. Applicant respectfully points out that Hermann teaches away from the instant application. Specifically, Hermann is directed to establishing a secure session between devices to provide cryptographic means **to prevent an eavesdropper from learning the contents of the messages** between the devices (see Hermann, paragraph [0026], "*the unidirectional wireless communication channel can ensure that only the target device receives the initial-sequence. ...no other parties can eavesdrop and receive the initial-sequence*," and paragraphs [0047]-[0054], which describes the technique for establishing a secure session).

In contrast, the present invention teaches establishing communication through a preferred communication channel that **does not require being resistant to eavesdropping**. More specifically, **an attacker can eavesdrop the transmissions on the preferred channel, so long as the attacker cannot transmit on the preferred channel without being detected** (see paragraphs [0078] of the instant application). The authenticity property of the preferred channel ensures that an eavesdropper that detects the commitment or keys sent across the preferred channel is not able to demonstrate possession of the corresponding

private key, and therefore is unable to affect communication between the legitimate parties.

This is beneficial because it creates a simple-to-establish credential provisioning procedure between the two communication devices without using complicated verification procedures. There is nothing within Hermann, either explicit or implicit, which suggests establishing communication between two devices using a preferred communication channel that does not require being resistant to eavesdropping.

Accordingly, Applicant maintains the amendments made to independent claims 1, 10, and 19 during the previous office action response which clarify that the present invention provides a technique, that allows two devices to establish communication **using a preferred communication channel that does not require being resistant to eavesdropping**. These amendments find support in paragraph [0078] of the instant application. No new matter has been added.

Hence, Applicant respectfully submits that independent claims 1, 10, and 19 are in condition for allowance. Applicant also submits that claims 2-4, 6-9, and 28, which depend upon claim 1, claims 11-13, 15-18, and 29, which depend upon claim 10, and claims 20-22, 24-27, and 30, which depend upon claim 19, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By /Shun Yao/
Shun Yao
Registration No. 59,242

Date: 15 August 2007

Shun Yao
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
Fax: (530) 759-1665
Email: shun@parklegal.com